Amendments to the Claims

We claim:

1. (original) A method carried out in a computer for providing periodic verification of the computer during requests from the computer to a second computer over a communications system, the method comprising:

establishing an authentication handshake with the second computer; and

periodically sending messages to the second computer,

wherein the second computer services the requests if the messages are valid and are received within a predetermined time interval.

2. (original) The method of Claim 1 wherein the authentication handshake comprises an exchange of a session key and a sequence value.

3. (original) The method of Claim 2 wherein the messages further comprise the session key and the sequence value.

4. (original) The method of Claim 3 wherein the session key and the sequence value are processed through a one-way hash function.

5. (original) The method of Claim 1 wherein the requests are to send data.

6. (original) The method of Claim 1 wherein the requests are to receive data.

7. (original) A method carried out in a computer for providing periodic verification of a second computer during requests from the second computer to the computer over a communications system, the method comprising:

establishing an authentication handshake with the second computer;

periodically receiving messages from the second computer; and

servicing the requests if the messages are valid and are received within a predetermined time interval.

8. (original) The method of Claim 7 wherein the authentication handshake comprises an exchange of a session key and a sequence value.

9. (original) The method of Claim 8 wherein the messages further comprise the session key and the sequence value.

10. (original) The method of Claim 9 wherein the session key and the sequence value are processed through a one-way hash function.

11. (original) The method of Claim 7 wherein the requests are to send data.

12. (original) The method of Claim 7 wherein the requests are to receive data.

13. (original) A computer storage system comprising:

a first computer coupled to a communications system; and

a second computer coupled to the communications system,

wherein:

the first computer establishes an authentication handshake with the second computer and periodically sends messages to the second computer;

the first computer sends requests to the second computer; and

the second computer services the requests if the messages are valid and are received within a predetermined time interval.

14. (original) The system of Claim 13 wherein the authentication handshake comprises an exchange of a session key and a sequence value.

15. (original) The system of Claim 14 wherein the messages further comprise the session key and the sequence value.

16. (original) The system of Claim 15 wherein the session key and the sequence value are processed through a one-way hash function.

17. (original) The system of Claim 13 wherein the requests are to send data.

18. (original) The system of Claim 13 wherein the requests are to receive data.

19. (original) A computer storage system comprising:

a first computer coupled to a communications system; and

a second computer coupled to the communications system,

wherein:

the first computer establishes an authentication handshake with the second computer and periodically receives messages from the second computer; and

the first computer receives requests from the second computer and services the requests if the messages are valid and are received within a predetermined time interval.

20. (original) The system of Claim 19 wherein the authentication handshake comprises an exchange of a session key and a sequence value.

21. (original) The system of Claim 20 wherein the messages further comprise the session key and the sequence value.

22. (original) The system of Claim 21 wherein the session key and the sequence value are processed through a one-way hash function.

23. (original) The system of Claim 19 wherein the requests are to send data.

24. (original) The system of Claim 19 wherein the requests are to receive data.

25. (original) A method carried out in a computer for providing periodic verification of at least two second computers during requests from the at least two second computers to the computer over a communications system, the method comprising:

establishing authentication handshakes with each of the at least two second computers;

periodically receiving messages from the at least two second computers, wherein the messages are different from each other; and

servicing the requests from the at least two second computers if their corresponding messages are valid and received within a predetermined time interval.

26. (original) The method of Claim 25 wherein the authentication handshakes comprise exchanges of at least two session keys and at least two sequence values.

27. (original) The method of Claim 26 wherein the messages further comprise the at least two session keys and the at least two sequence values.

28. (original) The method of Claim 27 wherein the at least two session keys and the at least two sequence values are processed through a one-way hash function.

29. (original) The method of Claim 27 further comprising:

reading a table for information to use in determining expected messages for each of the at least two second computers, wherein the table includes identifiers associated with the at least

two second computers, session keys associated with the at least two second computers, and sequence values associated with the at least two second computers;

determining the expected messages for each of the at least two second computers; and

validating that the expected messages for each of the at least two second computers are identical to each of their corresponding messages from the at least two second computers.

30. (original) A method carried out in a computer for providing periodic verification of the computer during requests from the computer to a second computer over a communications system, the method comprising:

establishing an authentication handshake with the second computer, wherein the authentication handshake includes a session key and a sequence value; and

periodically sending messages to the second computer, wherein the messages include the session key and the sequence value,

wherein the second computer services the requests if the messages are valid and are received within a predetermined time interval.

31. (original) The method of Claim 30 wherein the requests are to send data.

32. (original) The method of Claim 30 wherein the requests are to receive data.

33. (original) A method carried out in a computer for providing periodic verification of the computer during requests from the computer to a second computer over a communications system, the method comprising:

establishing an authentication handshake with the second computer, wherein the authentication handshake includes a session key and a sequence value; and

periodically sending messages to the second computer, wherein the messages include the session key and the sequence value which are processed through a one-way hash function,

wherein the second computer services the requests if the messages are valid and are received within a predetermined time interval.

34. (original) The method of Claim 33 wherein the requests are to send data.

35. (original) The method of Claim 33 wherein the requests are to receive data.

36. (original) A method carried out in a computer for providing periodic verification of a second computer during requests from the second computer to the computer over a communications system, the method comprising:

establishing an authentication handshake with the second computer, wherein the authentication handshake includes a session key and a sequence value;

periodically receiving messages from the second computer, wherein the messages include the session key and the sequence value; and

servicing the requests if the messages are valid and are received within a predetermined time interval.

37. (original) The method of Claim 36 wherein the requests are to send data.

38. (original) The method of Claim 36 wherein the requests are to receive data.

39. (original) A method carried out in a computer for providing periodic verification of a second computer during requests from the second computer to the computer over a communications system, the method comprising:

establishing an authentication handshake with the second computer, wherein the authentication handshake includes a session key and a sequence value;

periodically receiving messages from the second computer, wherein the messages include the session key and the sequence value which are processed through a one-way hash function; and

servicing the requests if the messages are valid and are received within a predetermined time interval.

40. (original) The method of Claim 39 wherein the requests are to send data.

41. (original) The method of Claim 39 wherein the requests are to receive data.

42. (original) A computer-executable process stored on a computer-readable medium, the computer-executable process generating periodic verification of a computer during requests from the computer to a second computer over a communications system, the computer-executable process comprising:

code to establish by the computer an authentication handshake with the second computer, wherein the authentication handshake includes a session key and a sequence value; and

code to periodically generate and send messages to the second computer, wherein the messages include the session key and the sequence value which are processed through a one-way hash function.

43. (original) A computer-executable process stored on a computer-readable medium, the computer-executable process generating periodic verification of a computer during requests from a second computer over a communications system, the computer-executable process comprising:

code to establish by the computer an authentication handshake with the second computer;

code to periodically receive messages from the second computer messages; and

code to service the requests if the messages are valid and are received within a predetermined time interval.

44. (Currently Amended) The ~~method~~ computer-executable process of Claim 43 wherein the requests are to send data.

45. (Currently Amended) The ~~method~~ computer-executable process of Claim 43 wherein the requests are to receive data.

46. (original) A method carried out in an intelligent storage device for providing periodic verification of a computer during requests from the computer to the intelligent storage device over a communications system, the method comprising:

establishing an authentication handshake with the computer, wherein the authentication handshake includes a session key and a sequence value;

periodically receiving messages from the computer, wherein the messages include the session key and the sequence value which are processed through a one-way hash function; and

servicing the requests if the messages are valid and are received within a predetermined time interval.

47. (original) A method carried out in a computer for providing periodic verification of the computer during requests from the computer to an intelligent storage device over a communications system, the method comprising:

establishing an authentication handshake with the intelligent storage device, wherein the authentication handshake includes a session key and a sequence value; and

periodically sending messages to the intelligent storage device, wherein the messages include the session key and the sequence value which are processed through a one-way hash function,

wherein the intelligent storage device services the requests if the messages are valid and are received within a predetermined time interval.

48. (Previously Presented) A method to protect stored data, comprising:

receiving from a device verification information verifying the identity of the device;

verifying the validity of the verification information using common information known to the device and to the processor;

determining an authorization status of the device based on (1) the validity of the verification information and (2) a time the verification information is received by the processor;

receiving a request from the device to access the stored data; and

allowing the device to access the stored data based, at least in part, on the authorization status at the time the request is received.

49. (Previously Presented) The method of claim 48, comprising:

determining the authorization status of the device based on (1) the validity of the verification information and (2) whether the verification information is received during a predetermined time interval.

50. (Previously Presented) The method of claim 48, further comprising:

updating the common information; and

instructing the device to update the common information.

51. (Previously Presented) The method of claim 48, comprising establishing an initial authorization status of the device based on a predefined authentication process.

52. (Previously Presented) The method of claim 48, wherein the common information comprises a sequence value.

53. (Previously Presented) The method of claim 52, wherein the common information further comprises a session key.

54. (Previously Presented) The method of claim 53, wherein the verification information comprises a verification value.

55. (Previously Presented) The method of claim 54, further comprising:

updating the sequence value according to a first predetermined algorithm to generate an updated value;

applying a second predetermined algorithm to the updated value to generate an expected value;

comparing the expected value to the verification value; and

determining the verification value to be valid if the expected value is the same as the verification value.

56. (Previously Presented) The method of claim 55, wherein the first predetermined algorithm comprises updating the stored value by a predetermined increment value.

57. (Previously Presented) The method of claim 55, wherein the second predetermined algorithm comprises applying a hash function to the updated value and the session key to generate the expected value.

58. (Previously Presented) The method of claim 54, comprising:

retrieving an expected value from a table;

comparing the verification value to the expected value; and

determining the validity of the verification value based on the comparison.

59. (Previously Presented) The method of claim 48, further comprising:

performing one or more times, by a processor, the following:

the receiving from a device verification information verifying the identity of the device;

the verifying the validity of the verification information using common information known to the device and to the processor; and

the determining an authorization status of the device based on (1) the validity of the verification information and (2) the time the verification information is received by the processor.

60. (Previously Presented) The method of claim 48, further comprising:

ceasing to service requests received from the device when verification information is not received by the processor within a predetermined time interval.

61. (Previously Presented) The method of claim 48, wherein the verification information is received by the processor within a heartbeat message.

62. (Previously Presented) A method to protect stored data, comprising:

providing authentication information to a processor responsible for managing data processing requests relating to stored data;

performing, at least once during one or more time intervals having predetermined durations, the following actions:

retrieving from memory a value previously received from the processor;

applying a predetermined algorithm to the value to generate an encoded value; and

transmitting the encoded value to the processor; and

transmitting to the processor at least one data processing request relating to the stored data.

63. (Previously Presented) The method of claim 62, wherein the predetermined algorithm comprises updating the value by a predetermined increment value.

64. (Previously Presented) The method of claim 63, wherein the predetermined algorithm further comprises encoding the updated value using a session key previously provided by the processor.

65. (Previously Presented) The method of claim 64, wherein the predetermined algorithm comprises a hash function.

66. (Previously Presented) The method of claim 62, further comprising:

receiving an acknowledgment message from the processor;

in response to the acknowledgment message, updating the value.

67. (Previously Presented) A system to protect stored data, comprising:

a device configured to:

transmit verification information verifying the identity of the device; and

transmit at least one request to access stored data; and

a processor configured to:

receive from the device the verification information;

verify the validity of the verification information using common information known to the device and to the processor;

determine an authorization status of the device based on (1) the validity of the verification information and (2) a time the verification information is received by the processor;